

[View in a browser](#)

[VFC Homepage](#)

[Shield Homepage](#)

[Shield Products](#)

[Online Resources](#)

[Report SAR](#)



CyberAware

Awareness Through Information Sharing

Incidents/Articles of Note:

- The biggest cyber hacks of 2021
- Ransomware attack shuts down computer systems for Virginia legislative agencies
- Mass spyware campaign targets thousands of ICS computers around the world
- Virginia Museum Shuts Down Website Amid IT Breach
- US government to offer up to \$5,000 'bounty' to hackers to identify cyber vulnerabilities
- Hackers launch over 840,000 attacks through Log4J flaw
- Bugs in billions of WiFi, Bluetooth chips allow password, data theft
- Northam proposes \$60M for cyber as Virginia agencies deal with hacks

- Tools and Resources -



Resource | DHS CISA

Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom have released a [joint Cybersecurity Advisory](#) in response to multiple vulnerabilities in Apache's Log4j software library.

Malicious cyber actors are actively scanning networks to potentially exploit [CVE-2021-44228](#) (known as "Log4Shell"), [CVE-2021-45046](#), and [CVE-2021-45105](#) in vulnerable systems. According to public reporting, Log4Shell and CVE-2021-45046 are being actively exploited.

This advisory expands on [CISA's previously published guidance](#), drafted in collaboration with industry members of CISA's [Joint Cyber Defense Collaborative \(JCDC\)](#), by detailing recommended steps that vendors and organizations with information technology, operational technology/industrial control systems, and cloud assets should take to respond to these vulnerabilities.

[View Resource](#)



Resource | CISA

Immediate Steps to Strengthen Critical Infrastructure against Potential Cyberattacks

In light of persistent and ongoing cyber threats, CISA urges critical infrastructure owners and operators to take immediate steps to strengthen their computer network defenses against potential cyberattacks. CISA has released [CISA Insights: Preparing For and Mitigating Potential Cyber Threats](#) to provide critical infrastructure leaders with steps to proactively strengthen their organization's operational resiliency against sophisticated threat actors, including nation-states and their proxies.

CISA encourages leadership at all organizations—and critical infrastructure owners and operators in particular—to review the [CISA Insights](#) and adopt a heightened state of awareness.

[View Resource](#)

This is an **open-source** product. Redistribution is encouraged.



**View Virginia Fusion
Center Homepage**

[Click Here](#)



**Observe Suspicious
Activity?**

[Report Online](#)

Not a VFC Shield Member?

[Join Today](#)

Virginia Shield Coalition

"Awareness Through Information Sharing"





Need Help with this Email?

[View in a browser](#)

Useful Links

[VFC Fusion Site](#)

VFC Shield

Shield Homepage

*"Awareness Through Information
Sharing"*

All Products

Report SAR

Email Coordinator

The opinions or conclusions of the authors reflected in the open source articles and resources is not endorsed and/or does not necessarily reflect the opinion of the Virginia Fusion Center. The sources have been selected to provide you with event information to highlight available resources designed to improve public safety and reduce the probability of becoming a victim of a crime.
